LEGALIDADE E AUTENTICIDADE DE DOCUMENTOS em MEIO DIGITAL

CERTIFICAÇÃO DIGITAL E ASSINATURA DIGITAL: A EXPERIÊNCIA DA USP

Conceitos e problemas envolvidos

Agenda

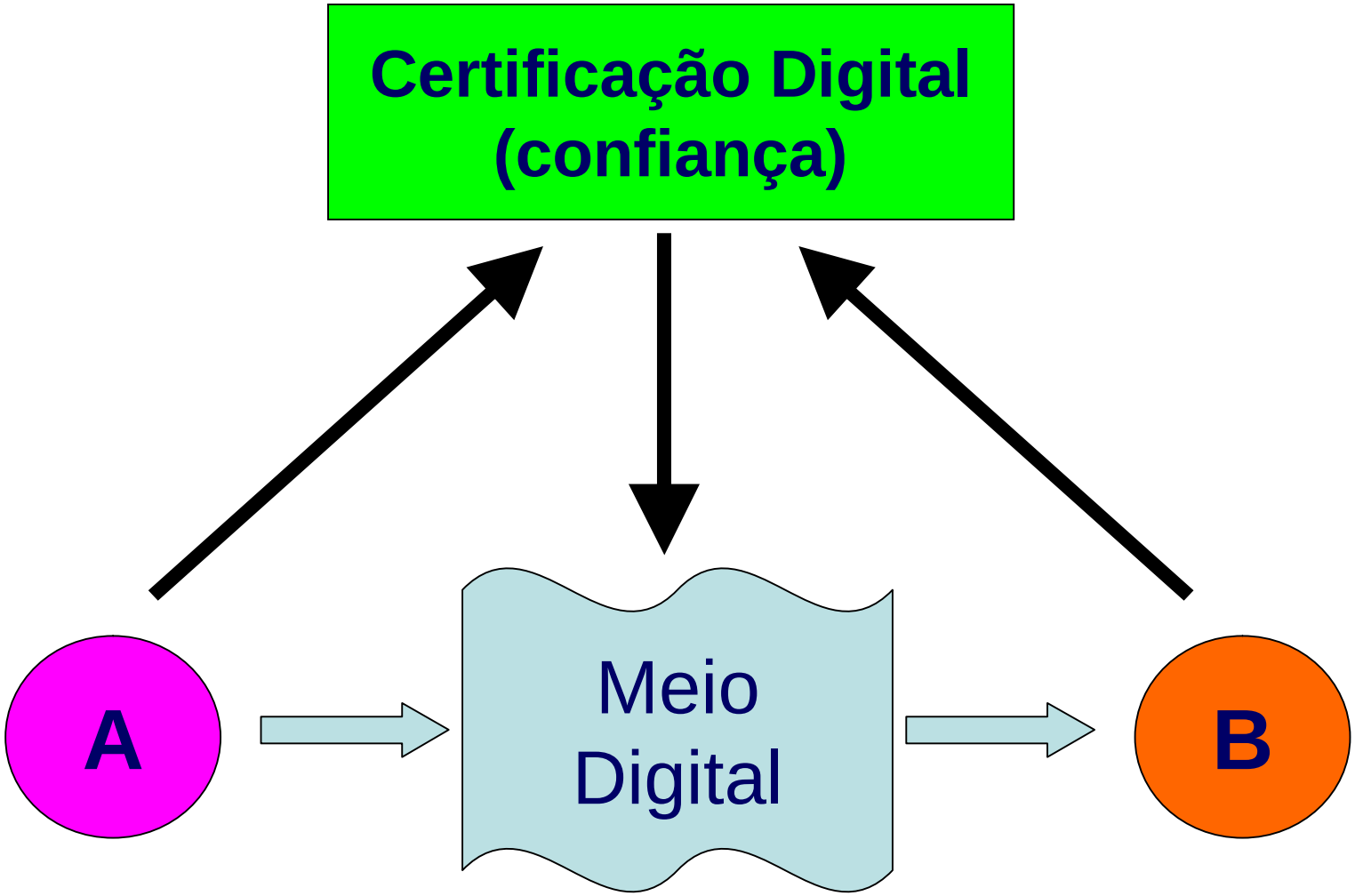
- Histórico
- Conceitos
- Aplicações na USP
- Recomendações

Assinatura e Certificação Digital

Objetivo => garantir a equivalência funcional legal entre documentos analógicos e digitais

Fragilidades do meio digital

- Sites clonados
- E-mails forjados
- Arquivos adulterados
- Dificuldade de comprovar fraudes
- Dificuldades com autenticidade, integridade, sigilo, tempestividade


Certificação Digital
(confiança)
A
Meio
Digital
B

Certificação Digital

- Aspectos Jurídicos
- Aspectos Tecnológicos
- Aspectos Culturais

Aspectos Jurídicos

- **equivalência funcional entre a assinatura digital e uma assinatura manuscrita lavrada em papel**

- **eficácia probatória: verificação a qualquer momento (acessibilidade) se o conteúdo assinado foi alterado (integridade) e garantir a identificação do assinante (autenticidade)**

Aspectos Tecnológicos

- Disseminação da tecnologia
- Garantias oferecidas
- Aplicações com baixo custo

Aspectos Culturais

- Cultura do papel
- Falta de confiança na tecnologia
- Benefícios não visíveis
- Tradicional resistência à mudança
- Desconforto com o mundo digital
- Não abrangência (exclusão digital)
- Custos

Conceitos

Mundo Digital x Analógico

- Assinatura: marca pessoal empregada para designar autoria, visto ou aprovação
- Autenticação: ato pelo qual algo é reconhecido como verdadeiro
- Certificação: afirmação de certeza

Mundo Digital x Analógico

- Mundo analógico (papel)
  - Conteúdo escrito é visível (leitura)
  - Original é o primeiro suporte
  - Suporte de difícil duplicação
  - Assinatura (marca) faz parte do conteúdo

- Mundo digital
  - Conteúdo acessível (localizável, interpretável)
  - Original é o *"formato original"* (integridade)
    - documentos digitalizados ou impressos são cópias
    - cópias de arquivos são originais
  - Assinatura (autenticidade + integridade)

- **Autenticidade**

  garantia da identificação e associação do autor ao conteúdo => não repúdio

- **Integridade**

  possibilidade de verificar a qualquer momento se o conteúdo assinado está íntegro (peritos fazem isso no papel)

Assinatura no mundo digital

- Digitalizada
- Baseada em biometria
- Digital

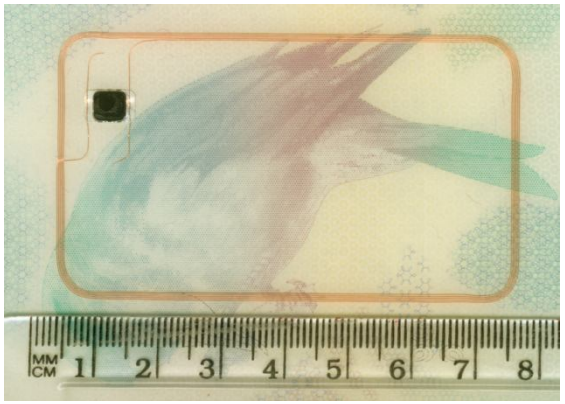
Assinatura Digitalizada

- Digitalização da assinatura manuscrita
- Pode ser obtida de modo estático ou dinâmico
- Imagem
- Seqüência de bits que pode ser colada e copiada
- Não pode garantir integridade nem autenticidade do conteúdo

Assinatura baseada em biometria

- Utiliza padrões biométricos (digital, íris, voz, DNA, geometria do rosto etc.)
- Método de identificação
- Controle de acesso lógico (senhas) e físico (catracas, portas)
- Seqüência de bits que pode ser colada e copiada
- Não pode garantir integridade nem autenticidade do conteúdo

Passaporte Biométrico (e-Passporte)



Fonte: Wikimedia Commons

Assinatura digital

- Equivalência funcional em relação a assinatura manuscrita
- Possibilita verificar se o conteúdo assinado foi alterado (integridade)
- Pode garantir a identificação do assinante (autenticidade) em conjunto com Certificação Digital
- Garante vínculo lógico entre um documento e a assinatura

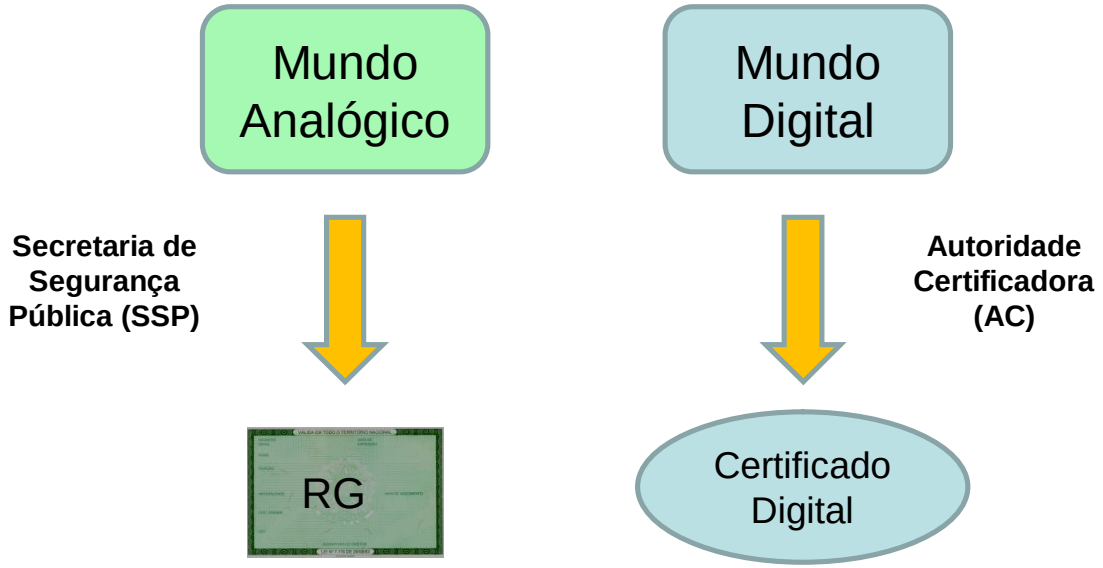
Assinatura Digital

é diferente de

Assinatura Digitalizada

Certificação Digital

Atividade de reconhecimento em meio eletrônico que se caracteriza pelo estabelecimento de uma relação única, exclusiva e intransferível entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação. Esse reconhecimento é inserido em um certificado digital por uma autoridade certificadora.

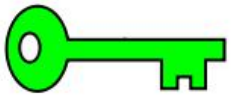


Certificado Digital

Documento emitido e assinado digitalmente por uma autoridade certificadora, que contém dados que identificam seu titular e o relaciona à sua respectiva chave-pública.

- arquivo que contém informações de identificação do titular
- Documento eletrônico que identifica pessoas. Espécie de “RG eletrônico”
- atesta a titularidade de uma chave criptográfica
- a vinculação entre o certificado e o titular é garantida pela Autoridade de Registro
- tem prazo de validade (a evolução das técnicas de criptoanálise pode invalidar um Certificado)

- **Chave Privada** 
  - arquivo de uso privativo do proprietário da chave
  - utilizado para cifrar (criptografar) mensagens no processo de assinatura eletrônica
  - pode ser armazenado no computador através de software de utilização ou ainda estar em outro meio físico como um CD, pen-drive ou token
  - normalmente a chave privada é protegida por uma senha
  - jamais deverá ser enviada ou copiada para outras pessoas

- **Chave Pública** 
  - arquivo de acesso público
  - usada para descriptografar uma mensagem criptografada por uma chave privada ou,
  - criptografar uma mensagem que só poderá ser descriptografada pela chave privada
  - no contexto da assinatura digital, é usada para a autenticação

- **Autoridade Certificadora (AC)**

  – Entidade de confiança do solicitante do Certificado Digital para garantir a identidade dos envolvidos numa operação eletrônica.

- **Autoridade de Registro (AR)**

  – Entidade responsável pela identificação presencial do solicitante de um Certificado Digital.

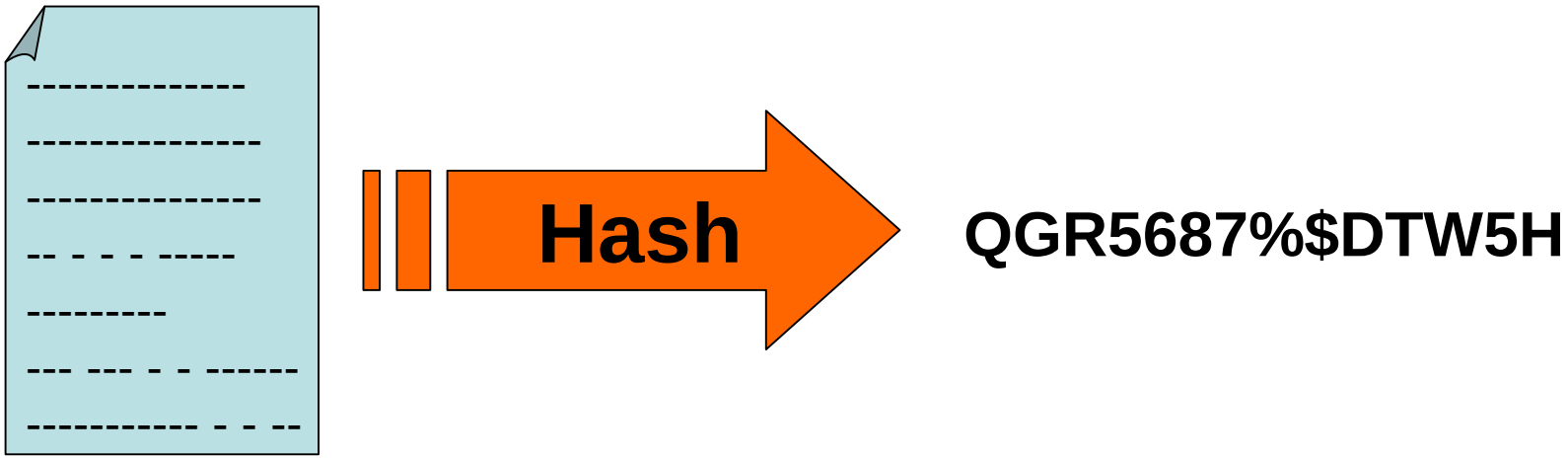
Ciclo de vida do Certificado Digital

- **Inicialização**
  - Cadastramento do titular
  - Geração do par de chaves
  - Criação / Entrega / Publicação
- **Utilização**
  - Busca / Validação
- **Cancelamento**
  - Vencimento (fim da validade)
  - Revogação (comprometimento da chave privada, comprometimento da chave da AC, alteração de dados do titular, fim do propósito)
  - Arquivamento da chave

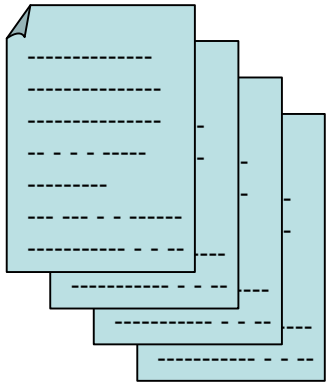
Tempestividade

- possibilidade de comprovar que um evento eletrônico ocorreu em um determinado instante
- não é sinônimo de temporalidade
- Autoridade de Tempo (Observatório Nacional)
- Carimbo de tempo
- Selo cronológico digital (estampilha temporal)
  - comprova que um documento existia num determinado instante (data e hora)
  - que o documento não sofreu alteração desde então
  - que o documento não foi substituído por outro

Resumo de mensagem



Resumo de mensagem

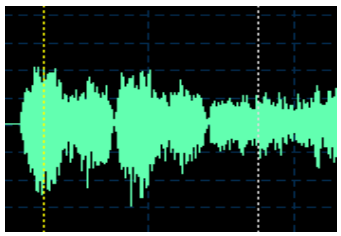


Hash

IUIY¨¨%#$%$DTW5H

Hash

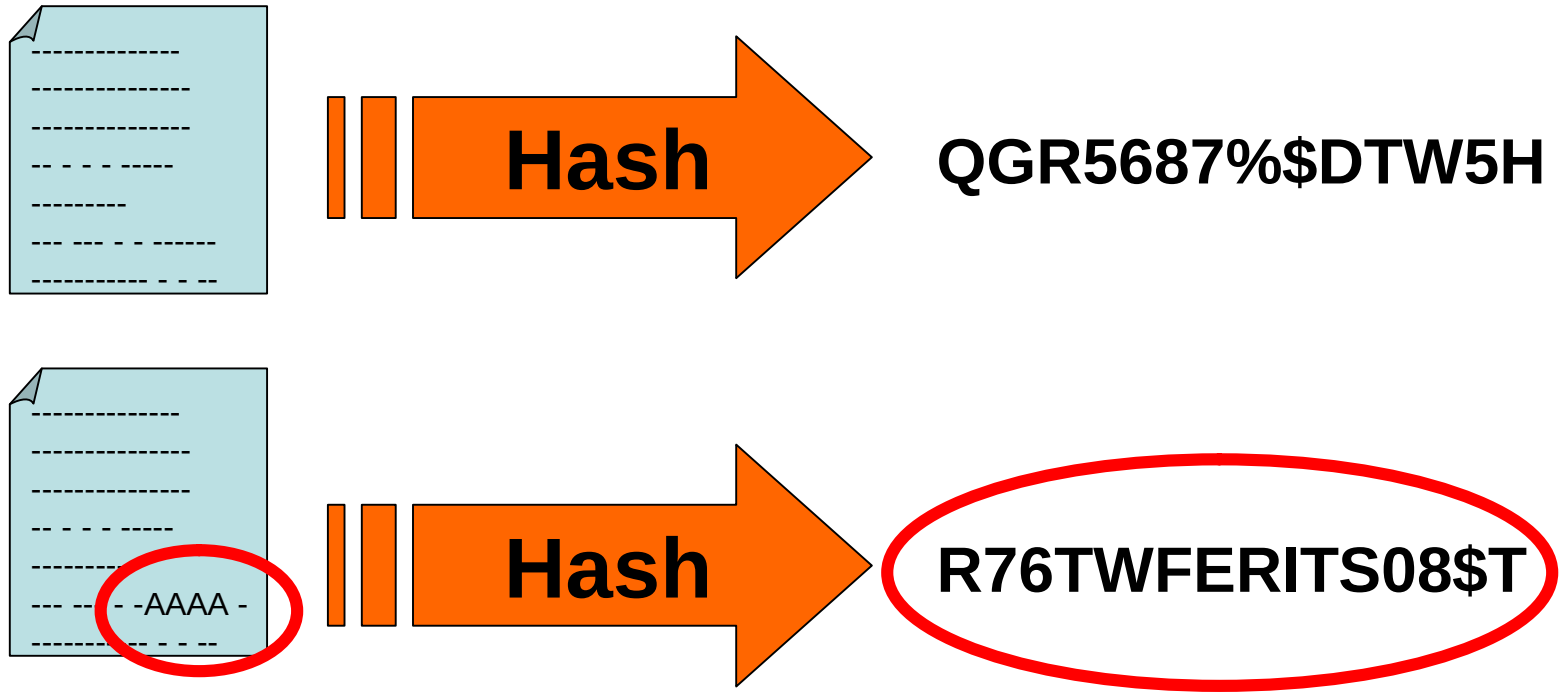
OEYK$#45DTW436



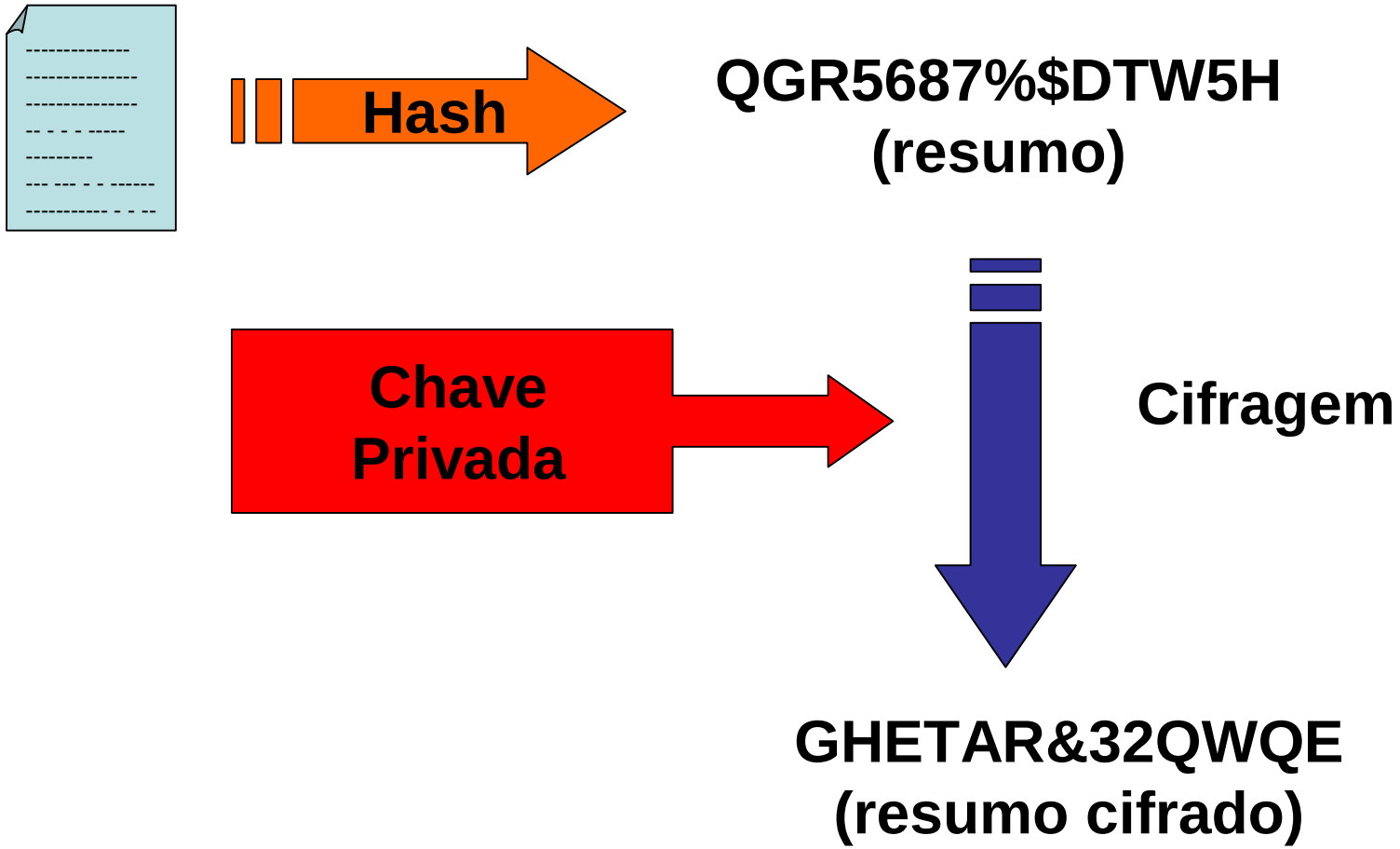
Hash

PO6TR$#POL8F45

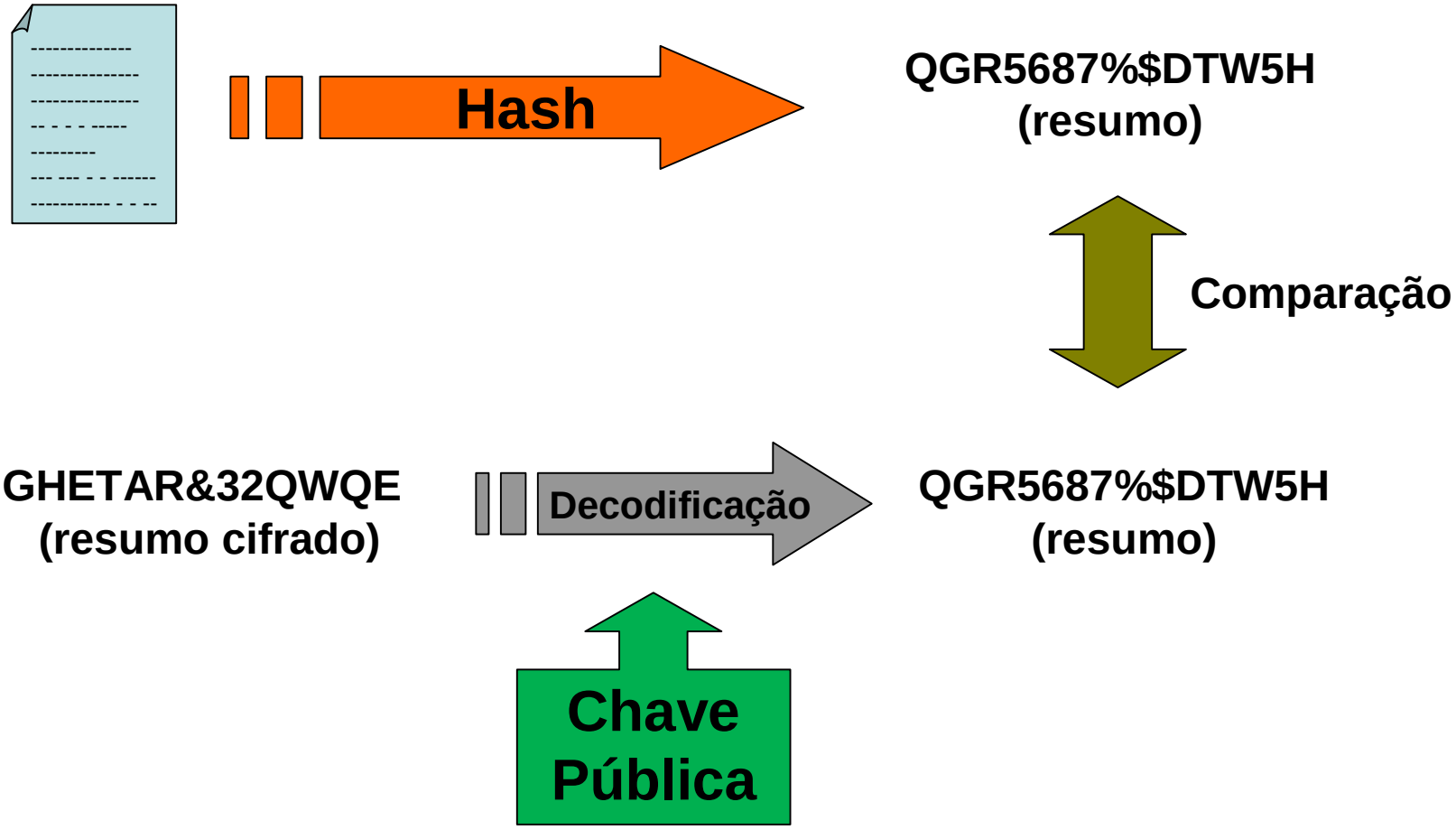
O resumo de mensagem é único



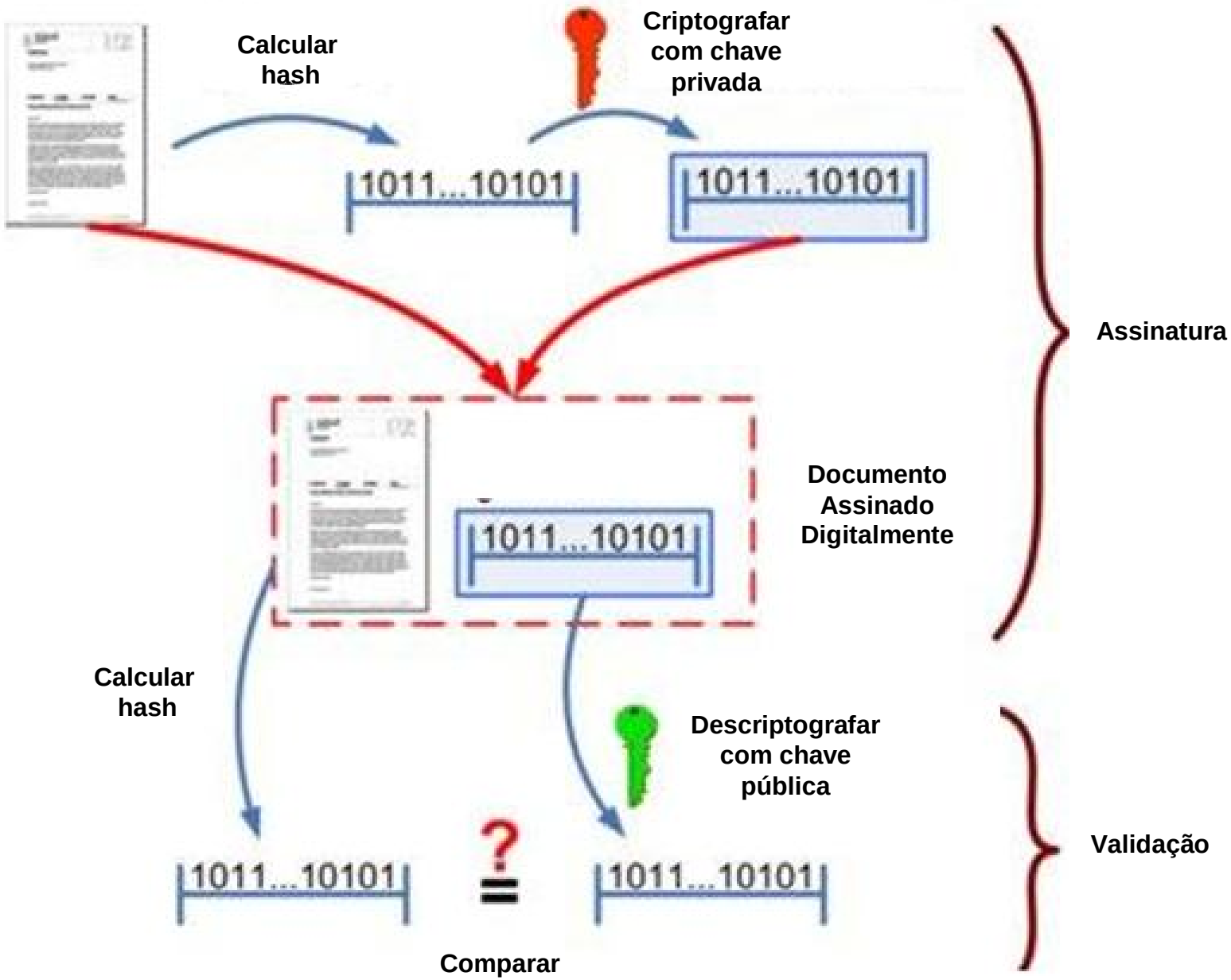
Assinatura Digital



Validação da Assinatura Digital



- **Processo de Assinatura Digital**
  - geração do resumo de mensagem
  - criptografia do resumo com a chave privada
- **Processo de validação**
  - geração do resumo de mensagem a partir do texto recebido
  - descriptografia do resumo recebido com a chave pública
  - comparação dos resumos (recebido e gerado localmente)


Calcular hash
Criptografar com chave privada
1011...10101
1011...10101
Assinatura
Documento Assinado Digitalmente
1011...10101
Calcular hash
Descriptografar com chave pública
1011...10101
?
1011...10101
Validação
Comparar

Equivalência funcional

Mundo analógico

texto + marca pessoal => doc. Assinado

Mundo digital

resumo + chave pessoal => doc. Assinado

QGR5687%$D TW5H **+**  **=>** **U*&YUI7TDP8**

Infra-estrutura de Chaves Públicas (ICP)

- sistema de confiança, no qual duas partes (pessoas ou computadores) confiam mutuamente em uma Autoridade Certificadora (AC) para verificar e confirmar a identidade de ambas as partes

- também conhecida com PKI (Public Key Infrastructure)

Infra-estrutura de Chaves Públicas (ICP)

- Criptografia assimétrica
  - chaves pública e privada
- Hash
- Assinatura Digital
  - Padrões
  - Processos de assinatura e verificação
- Certificação Digital
  - Autoridade Certificadora (AC)
  - Autoridade de Registro (AR)

ICP-Brasil

- Medida Provisória 2.200-2 de 24/08/2001
- modelo isolado (única AC Raiz) e hierarquizado
- AC-Raiz operacionaliza e audita as ACs abaixo, dela na hierarquia, mas não emite certificado para usuários finais
- Comitê Gestor como Autoridade de Políticas
- ITI (Instituto de Tecnologia da Informação) é a AC-Raiz

http://www.iti.gov.br

ICP-Edu

- ICP no âmbito acadêmico
- Grupo de Trabalho na Rede Nacional de Ensino e Pesquisa (RNP) envolvendo diversas universidades
- Disponibilização, sem custos e de maneira facilitada, de certificados digitais para alunos, professores, funcionários ou pesquisadores acadêmicos
- AC-Raiz na RNP
- Certificados da ICP-EDU não terão valor jurídico
- Características alinhadas ao ambiente acadêmico: experimentação, capacitação, domínio da tecnologia

Medida Provisória 2.200-2 de 24/08/2001

Artigo 10º - Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

§ 1º - As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei no 3.071, de 1 de janeiro de 1916 - Código Civil.

§ 2º - O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento

No Estado de São Paulo

- Decreto estadual 48.599 de 12/04/2004

Artigo 2º - Os serviços de certificação digital, descritos no anexo ao presente decreto, serão obrigatoriamente contratados com a Imprensa Oficial do Estado S.A . - IMESP, que atuará como Autoridade Certificadora - AC e Autoridade de Registro - AR, nos termos da normatização de regência

Tipos de Certificado

- **Assinatura (A1, A2, A3, A4)**
  - assinatura de documentos, transações eletrônicas, e-mail seguro
- **Sigilo (S1, S2, S3, S4)**
  - cifragem de documentos, mensagens, dados para garantir sigilo
- **Documentos com assinatura podem ser verificados mesmo com o extravio da chave privada => usa-se a chave pública**
- **Documentos com sigilo não podem mais ser acessados sem a chave privada**
- **Exigência do padrão X.509**

Tipos de Certificado

Tipo	Chave	Geração	Validade
A1 e S1	1024 bits	software	1 ano
A2 e S2	1024 bits	hardware	2 ano
A3 e S3	1024 bits	hardware	3 ano
A4 e S4	2048 bits	hardware	4 ano

Alguns Usos no Brasil

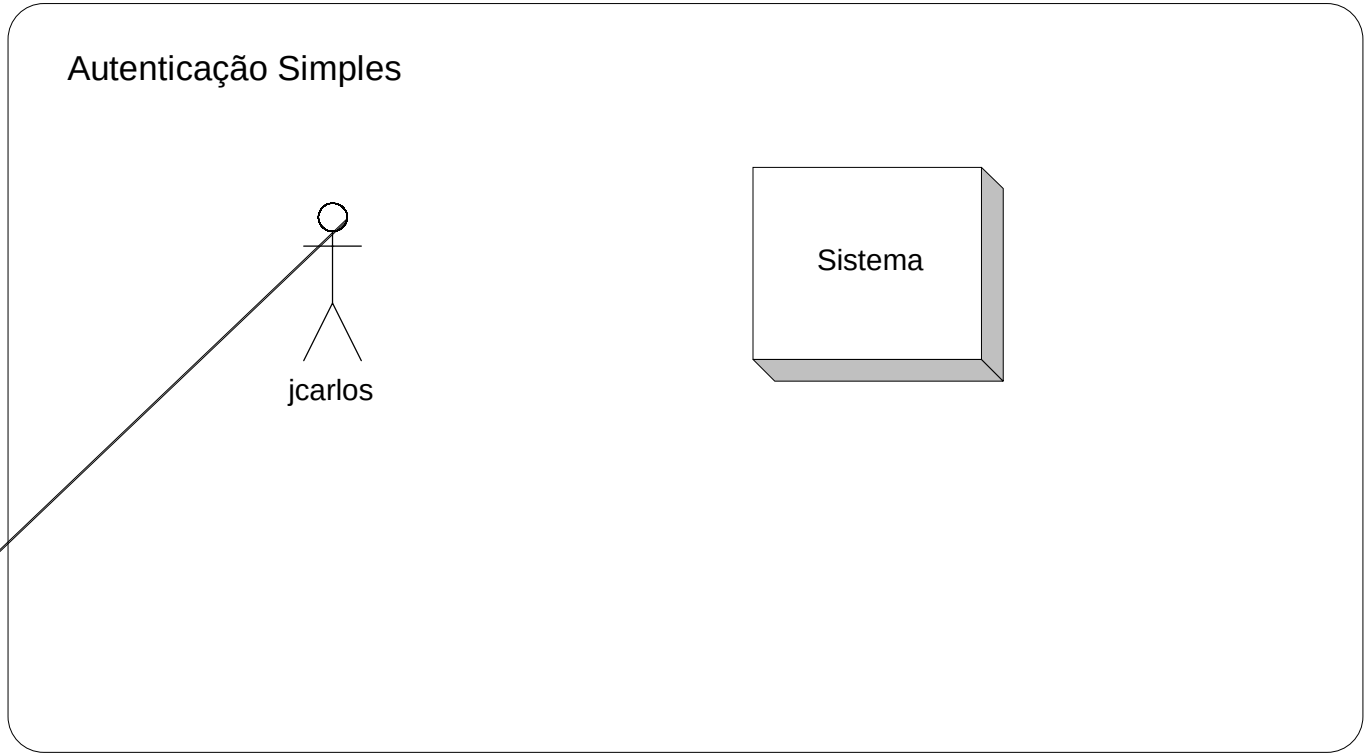
- e-CPF / e-CNPJ
- Sistema de Pagamentos Brasileiro
- Cartórios (fé pública em cópias eletrônicas)
- Receita Federal
- Trâmite interno entre Presidência da República e Ministérios
- Peticionamento eletrônico
- SEFAZ/SP

Aplicações na USP

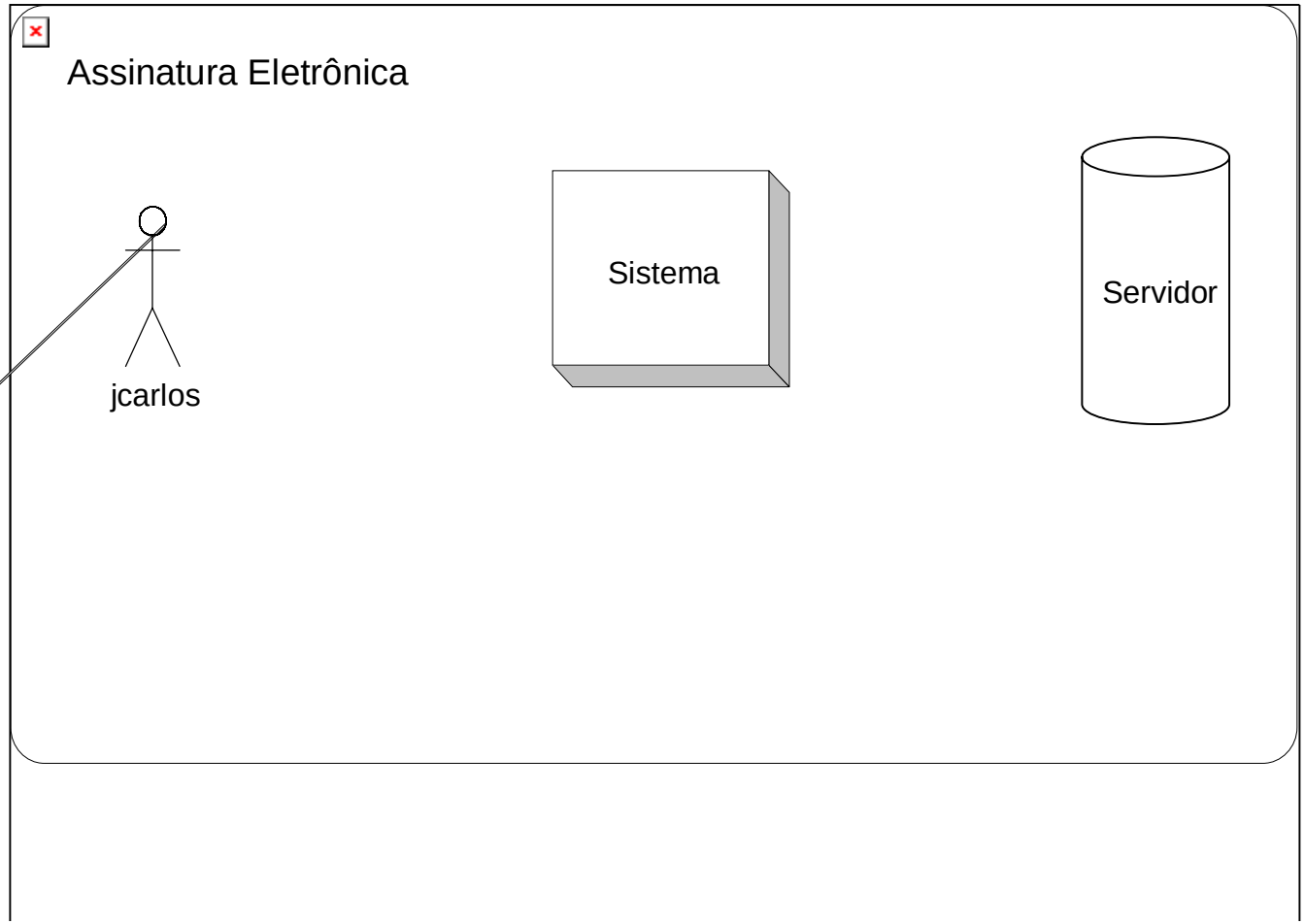
Aplicações na USP

- Documentos como históricos, atestados e certidões disponibilizados em meio digital
- Publicações
- Mensagens de correio eletrônico
- Autorizações
- Assinatura de documentos oficiais
- Assinatura de solicitações, requerimentos etc.
- Certificado de autenticidade de documentos e reproduções em meio digital

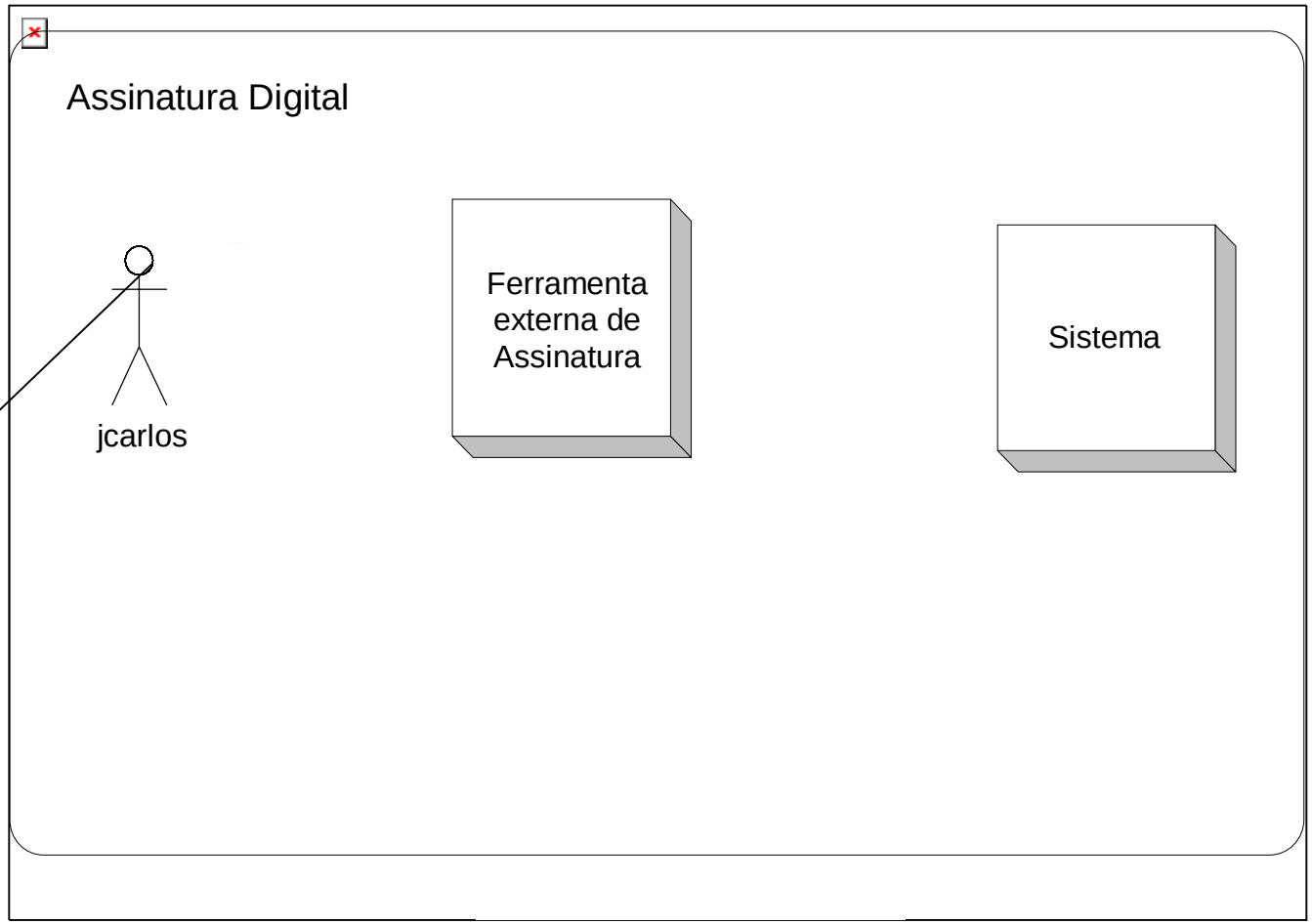
Autenticação simples (usuário/senha)



Assinatura eletrônica, gerenciada por servidor de conteúdo



Assinatura digital com ferramenta externa



Instrução Normativa APE/SAESP-1

Artigo 2º II

Arquivo digital - conjunto de bits que formam uma unidade lógica interpretável por computador e armazenada em suporte apropriado.

Artigo 8º

As mensagens de correio eletrônico e seus anexos são documentos arquivísticos digitais quando produzidas ou recebidas no exercício de função ou atividade do órgão ou entidade, e deverão integrar os programas de gestão arquivística de documentos, observando os Planos de classificação de documentos, aprovados pelo Arquivo Público do Estado.

Instrução Normativa APE/SAESP-1

Artigo 9º

Os documentos produzidos a partir de sistemas informatizados e bases de dados, gerados por órgãos e entidades no exercício de suas funções e atividades, e que tenham formas fixas e conteúdos estáveis, são considerados documentos arquivísticos digitais.

Artigo 24

Os riscos decorrentes da obsolescência tecnológica devem ser evitados com o monitoramento permanente dos avanços tecnológicos, ações rotineiras de manutenção e aplicação de técnicas de preservação digital comumente utilizadas, tais como migração, emulação, encapsulamento e conversão de dados.

Instrução Normativa APE/SAESP-1

Artigo 25

Os riscos decorrentes da dependência de fornecedor ou fabricante de software, hardware e formato devem ser evitados com a migração, com a utilização de soluções independentes e de padrões abertos de formatos de arquivo, de ampla aceitação por organismos oficiais, em âmbito nacional e internacional, e de recursos tecnológicos estáveis e consolidados no mercado.

Artigo 30

A assinatura e a certificação digitais devem utilizar infra-estrutura de chaves públicas, nos termos da lei, observadas as disposições do Decreto estadual 48.599, de 12-4-2004, que regula a contratação da prestação de serviços de certificação digital no âmbito da Administração Pública Estadual.

Recomendações para implantação

Recomendações

- Implantação gradativa da tecnologia
- Utilização de assinatura digital apenas onde estritamente necessário
- Projeto piloto
- Treinamento e Capacitação

Recomendações

- Projeto-piloto para assinatura, com escopo restrito
  - um sub-fluxo definido (recorte por processo)
  - um conjunto de documentos definido (recorte por conteúdo)
  - um número controlado de usuários, como, por exemplo, os usuários da área jurídica (recorte por usuários)
  - uma combinação de recortes onde um grupo de usuários atua sobre um conjunto definido de documentos em um ou mais sub-fluxos

Recomendações

- Treinamento e Capacitação

  – Palestras e workshops periódicos de divulgação dos aspectos da tecnologia

  – Treinamento dos usuários diretamente envolvidos no projeto piloto (disseminação)

  – Capacitação das equipes de informática, dos analistas de negócio e de suporte

Boas práticas

- Memorizar as senhas e não as compartilhar com ninguém a senha de acesso à chave privada
- Proteger o computador de acesso não-autorizado, mantendo-o fisicamente seguro
- Ao sair da mesa de trabalho, utilizar um protetor de tela com senha ou desligar o computador
- Usar produtos de controle de acesso ou recursos de proteção ao sistema operacional (como uma senha de sistema ou protetor de tela ativado por senha)
- Tomar medidas para proteger o computador de vírus
- Não utilizar como senhas dados pessoais, palavras dicionarizadas, datas ou somente números, pois são senhas de fácil descoberta

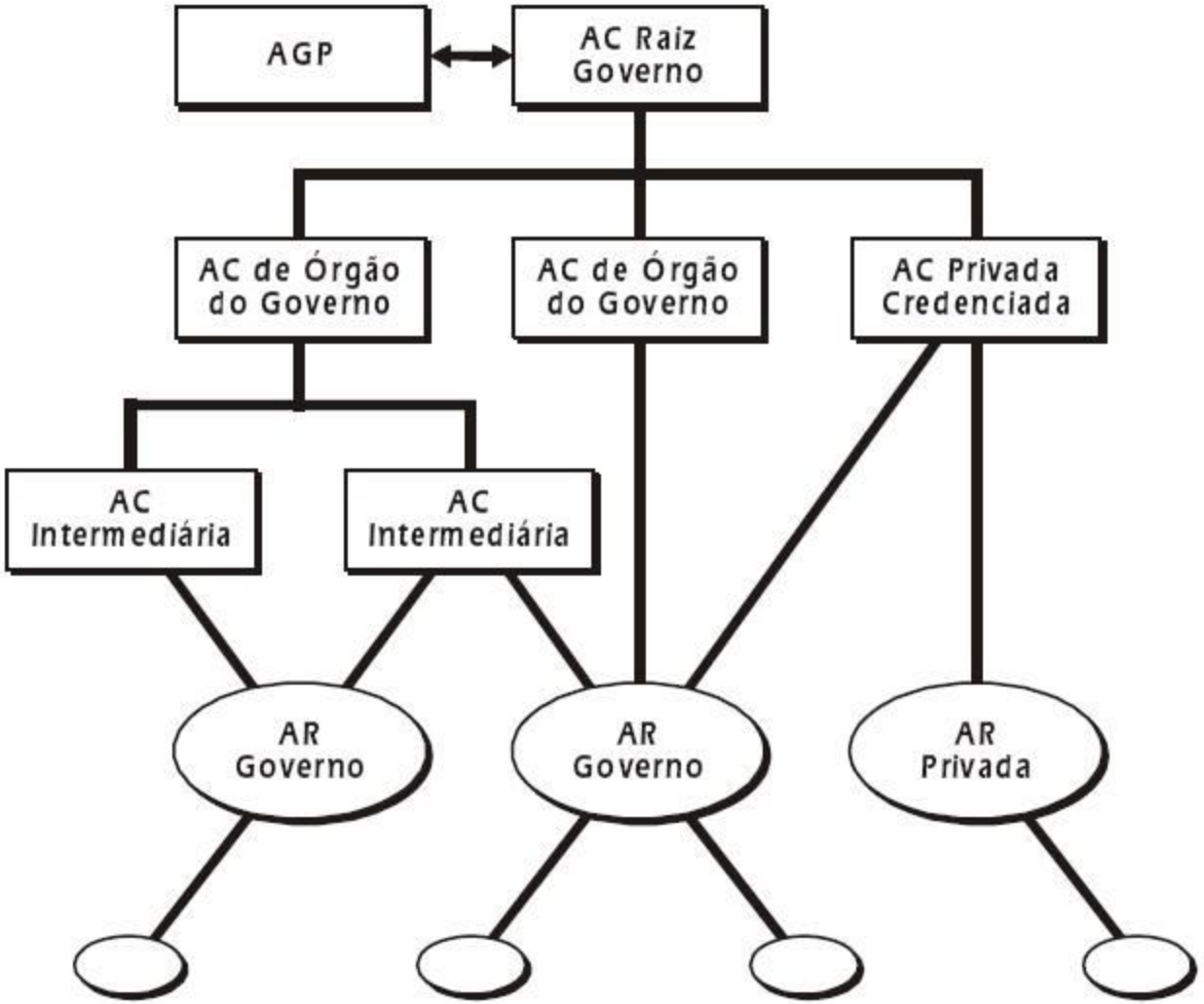
Boas práticas

- Em um local acessível a várias pessoas, como em um escritório, usar produtos de controle de acesso ou recursos de proteção do sistema operacional, como uma senha ou protetor de tela com senha
- Manter atualizados o sistema operacional e os aplicativos, pois versões mais recentes contêm correções que levam em consideração as vulnerabilidades mais atuais
- Não instalar o Certificado com a chave privada em computadores de uso público
- Em caso de suspeita de comprometimento da chave pública, seja por uma invasão sofrida no computador ou pelo surgimento de operações associadas ao uso da chave que não sejam de conhecimento do seu proprietário, a revogação do certificado deve ser solicitada o mais rápido possível à Autoridade Certificadora responsável pela sua emissão

Obrigado
pela participação!

Silvio de Paula
Departamento de Informática

depaula@usp.br


AGP
AC Raiz Governo
AC de Órgão do Governo
AC de Órgão do Governo
AC Privada Credenciada
AC Intermediária
AC Intermediária
AR Governo
AR Governo
AR Privada


MasterCard